FORESCOUT

The Benefits of Network Security Monitoring for Grid-Edge Devices

An in-depth analysis of how passive network security monitoring helps asset owners maintain an accurate, up-to-date asset inventory list, while also protecting the grid's edge from cyber threats.

Contents

Executive Summary

Among the many cybersecurity challenges associated with protecting the critical infrastructure power grid, two of the most challenging are maintaining an accurate asset inventory list and performing security monitoring of devices at the grid's edge. Not only are these capabilities fundamental to avoid regulatory fines upwards of a million dollars a day, as we saw recently when NERC issued a $10 million fine [1], but they also help ensure the overall security, safety, and reliability of the grid.

Often thought of as mutually exclusive, this paper shows that through advanced network security monitoring, asset owners can maintain, in real-time, an accurate and up-to-date asset inventory list while also protecting the grid's edge from cyber threats. By stepping through the different use cases for passive network security monitoring, the paper demonstrates how asset owners can reach a higher return on their investment in such a way that is technically, economically, and operationally feasible.

1. Introduction

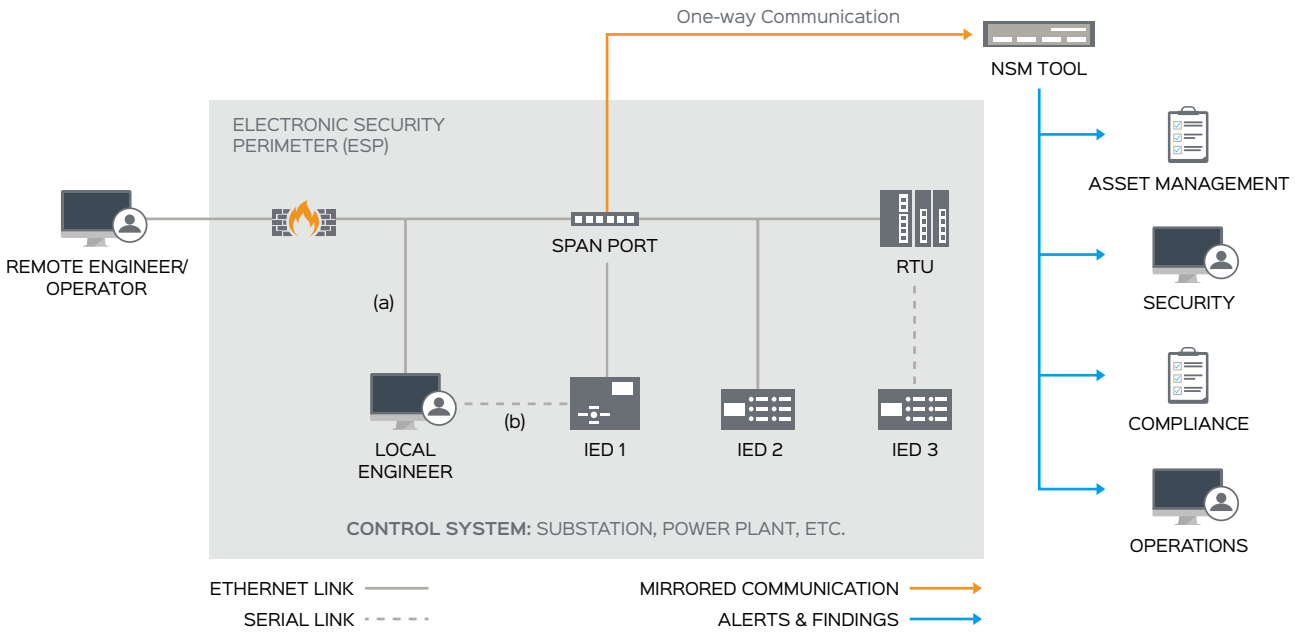
No one will argue securing critical infrastructure is important and a top priority for critical infrastructure asset owners. Asset owners are faced not only with evolving regulatory requirements such as the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards [2], but also growing attention from cybersecurity researchers and threat actors targeting industrial control system (ICS) technologies for their personal motivations. These motivations can vary from bringing awareness and helping the ICS community to compromising systems for financial gain or nation state objectives.

Originally, control system local area networks (LAN) were not connected to any Internet/Intranet connected devices.Though it didn't guarantee complete security, this did create the so-called air-gap, physically separating the devices from other Internet connected devices. However, for an increase in efficiency and remote monitoring/ control capabilities, the control system had to be integrated with other networks. The recommended network architecture for a control system combines the practices of IT security to the control system with the goal of a defense-in-depth secured environment [3]. However, simply applying IT security methods to ICS environments cannot be considered an end-all approach to cybersecurity, especially since solutions like firewalls can be misconfigured and have their own set of vulnerabilities.

> "Implementing power system automation control environments that are eliable, resilient, and secure is an interdisciplinary engineering challenge that involves multiple regulatory standards."

With the growth in and implementation of smart grid technologies there is often ambiguity in the roles and responsibilities associated with maintaining cyber-based technologies on the grid's edge. Electric utilities are often faced with asking themselves should the responsibility for power grid cybersecurity fall under the IT or telecom departments or should it be given to the power system engineers and integrators. In either case, effectively implementing power system automation control environments that are reliable, resilient, and secure is an interdisciplinary engineering challenge that involves multiple regulatory standards.

No matter who the threat actor is or what their motivations are. The first step in securing critical infrastructure is understanding what exists from an asset inventory perspective. Without knowing what exists and what you have to secure, all future threat modeling activities, strategy and roadmap development, or mitigation/remediation activities will be incomplete or less effective. Asset inventory is something both information technology (IT) and operational technology (OT) professionals can agree is not an easy task; historically speaking it has been especially labor intensive for ICS asset owners with "grid-edge" devices (or field devices), often requiring physical site visits. Grid-edge asset inventory difficulties are driven by the complex and aging heterogeneous environments most asset owners operate in that span across city, county, state, or country lines. Today, advancements in network security monitoring and protocol deep packet inspection allow asset owners to obtain real-time asset inventory information from devices communicating over serial or TCP/IP based communication channels by leveraging the built-in capabilities of grid-edge devices. This helps asset owners to not only manage their asset inventory, but also detect a variety of network, security, and operational based anomalies.



Example Network Topology Used for Evaluating the NSM Tool

2. Approach & Implementation

A. Approach

The developed approach is centered on the premise of being completely passive and non-intrusive to the control system environment. Using a managed network switch, a single port is configured as the span port. This span or mirroring port replays the communication traffic from all or a designated subset of the other ports on the switch. By placing a network security monitoring (NSM) tool on this span port, a detailed analysis of each communication packet is performed. This allows all inbound and outbound traffic to be monitored as well as the traffic between each intelligent electronic device (IED) at the grid's edge.

Selection of the devices and the NSM tool is based on an extensive review of the existing technologies available on the market today. While most microprocessor-based relays, remote terminal units, and managed switches can be implemented in this approach, not all control system NSM tools are created equal. Therefore, for completeness and so the reader can recreate the approach demonstrated, the NSM tool selected for this implementation is the eyeInspect (formerly SilentDefense) software solution by Forescout. The primary objective of this implementation is to passively derive as much information from sniffing the network as possible. To evaluate the effectiveness of the NSM tool selected, the extracted information is placed into one of four categories: asset management, security, compliance, and operations. Each category describes a business unit that is responsible for that aspect of the grid, and therefore will find value in that information. Additionally, some information may be classified into multiple categories. For instance, a failed login on IED1 is a security event that will also need to be noted for compliance. The NSM tool selected has the ability to export the findings via multiple formats for auditing purposes and for the tracking of asset information. This allows the extracted asset information to be imported into a system-wide asset management tool or, in the case of a cybersecurity event, into a security information and event management (SIEM) system.

B. Example Network Topology

The example network topology implemented is shown in Figure 1 and includes 3 protection relays, a remote terminal unit (RTU), a managed switch, and a firewall. All devices are logically defined within an electronic security perimeter (ESP). For servicing, engineers or technicians are typically allowed to enter the ESP and connect a transient cyber asset (TSA) to the IEDs [2]. Ethernet link (a) and serial link (b) show two options for directly communicating with such devices. For control, the standard control system protocols DNP3 and Modbus are used while for diagnostics each IED's web interfaces are enabled. Additionally, a vendor's specific protocol, which is an extension of the Telnet protocol, is used for communication between the RTU and IEDs. The managed switch is configured to mirror all TX and RX traffic on every port to a SPAN port. The NSM server has multiple network interfaces and the one connected to the span port is configured for RX only, while the SPAN port itself is configured for TX only.

C. Review of IED Settings and Configuration

As soon as the NSM tool came online, it began analyzing all the communication in the control system local area network including all ingress and egress traffic. Using this observed information, the NSM tool began to organize the observed devices into a network map according to the Purdue Model [5]. After just a few minutes, the NSM tool had accurately mapped all devices and protocols that where utilized over the network. To confirm this, a review of the IED settings files was performed. The IP information contained in these files was then used to confirm the specific whitelisted IPs that would be used to trigger an alarm in the NSM tool.

In addition to the IP settings information, the settings and configuration files of each IED was also examined to determine how the IED was alarming on cybersecurity events. Required by IEEE standard Std C37.240-2014, all IEDs are required to alarm on: unsuccessful login attempts, reboot, configuration changes, and firmware changes [6]. Similar to protection settings, these cybersecurity alarm settings are configured using the vendor's software. Another often overlooked, similarity is that these cyber alarms can be mapped to any binary point of a control system protocol (e.g. DNP3). Additionally, these and other cyber-related alarms were mapped in the IED and sent out via Syslog. With this information the NSM tool's built in scripting engine was used to passively detect and trigger an event alarm for multiple cyber-events, as described in detail in Section IV.

3. Asset Inventory Tracking

A. Overview

Maintaining an accurate and up-to-date baseline configuration often relies on a manual and handwritten process. A more efficient and less error-prone approach is to leverage the existing system to automatically observe and document changes as they are made. As noted in Section II, the example topology utilizes a vendor's slight variation of the Telnet protocol to communicate between the RTU and IEDs. Since this information is transmitted in plain text and is copied and replayed over the span port, the NSM tool is able to capture and analyze this information.

There are number of ways to achieve this functionality. Depending on the vendor of the IED, one option is to set the RTU to periodically poll the relay for its status, and the returned information will contain firmware version, model number, and the serial number of the device. However, based on the set poll rate, this information may only be polled every day or even every week. Therefore, a more responsive approach is to have the IED trigger a binary alarm upon a firmware change. After receiving the alarm, the RTU then polls the IED for the information identifying the new firmware version. This process then allows the NSM tool to immediately detect and log these changes. Once received by the NSM tool, the network map is updated to reflect the latest configuration change of the asset. This information can then be shared with a system-wide asset management tool.

The three example use cases below describe various ways an engineer or technician would be allowed to alter the firmware on an IED at the grid's edge. It's important to note that these actions could be performed by an attacker who has access to the network or by a malicious insider. The results are still the same and the developed approach will be able to capture, detect, and alert upon any firmware changes.

B. Example Use Cases Demonstrated

1. Remote engineer upgrades firmware on IED 1: There are several applications that may permit a remote engineer to have interactive access to an IED. This access allows the engineer to perform any number of commands as though he was physically at the device. Depending on how this remote access is configured, he could be allowed to communicate directly to the IED, or the RTU can be configured as an access point router.

2. Local engineer upgrades IED 2 firmware via Ethernet connection: If the previous use case is not allowed, an engineer or technician may be required to travel to the site to perform the necessary maintenance. While locally in the control house or plant, the engineer plugs into the network switch using an approved transient cyber asset [2] and logically connects to the IED. Once connected the engineer runs the upgrade command and uploads the firmware to the IED.

3. Local engineer upgrades IED 3 firmware via direct serial connection: The last use case is unique, since it requires some additional programming in the RTU in order to fully capture the upgrade. Unlike the other examples, this communication is not being performed over the network, and therefore will not be captured. Additionally, the polling of the device is being performed via a serial connection between the RTU and the relay. This polling is therefore also not being captured by the NSM tool. The solution here is to tell the RTU to log the firmware change of IED3 and all associated information to Syslog. This way when the updated asset information is placed on the network, the parsing feature of the NSM tool is still able to capture and log the event.

C. Vulnerability Identification

By having an accurate representation of the current firmware version installed on each device, the NSM tool was able to identify known vulnerabilities that are associated with that version of the firmware, protocols, and detected software. These vulnerabilities are based on the common vulnerability enumeration (CVE) standard and have an associated risk score identifying the impact that vulnerability could have to the system. This information can be used to determine when the device needs servicing. This ability greatly reduces the potential attack surface and helps ease the burden associated with meeting a number of compliance and maintenance requirements.

4. Security Monitoring

A. Overview

Network security monitoring (NSM) is a long time best cybersecurity practice of collecting, analyzing, and escalating indications of compromise. NSM in ICS networks is quickly gaining traction because that it can be accomplished without impacting the underlying OT systems, since no new traffic or communications are being introduced. With all network traffic being captured, the ICS NSM technology can leverage its deep packet inspection capabilities to completely parse an ICS protocol. This provides a complete understanding of what activity is occurring in real-time. Through these capabilities and added situational awareness, asset owners can reduce mean time to detection, response, and recovery for any cyber incidents occurring in ICS networks. Additionally, it provides both IT and OT incident responders the ability to obtain network packet captures containing the exact packets and messages related to an incident, resulting in a concise audit trail. By having an understanding of the control system protocols, the ICS NSM technology was able to automatically:

- Derive a network whitelist, including ICS/SCADA protocol specific function codes
- Derive a ICS/SCADA protocol whitelist including process values (binary or analog)
- Derive the role the device is performing in the industrial control system
- Create a network map with all the network flows between devices
- Detect known network-based indicators of compromise from malware or malicious campaigns
- Alert when operational thresholds are reached
- Extract device health information and alert when non-optimal conditions exist

B. Example Use Cases and Scenarios Tested

1. **Rogue device joins ICS network:** With all approved devices accurately mapped and placed in the Purdue model, this essentially creates a whitelist of devices that are approved to talk to one another. Any devices that connect to the network will automatically be captured by the NSM tool.

2. **Identify network communication failures:** More of an operational aspect of the grid, the examined NSM tool was able to determine when communication between devices ceases. This capability can be extremely valuable since it can help diagnose a broken link or down interface.

3. **Unauthorized device sends ICS/SCADA operate command:** With the whitelisted map created and since the tested NSM tool understands control system protocols, the tool was able to successfully detect when an unauthorized device initiates a command to a grid-edge device. In this case, the tool was able to learn the master-slave relationships of the network devices, and therefore become capable of detecting anomalies.

4. **Failed or successful remote or local logins into an RTU or IED:** The implemented devices were configured to sound an alarm upon either a successful or failed login. These alarms were then detected by the NSM tool.

5. **Use of default passwords:** By detecting the MAC address of each device on the network, the NSM tool is able to determine the specific manufacturer of that device. Using a built-in database of vendor utilized default passwords, the NSM tool compares detected username and password pairs to this database. Whenever a match is found a notification is produced identifying the networked device that has default username and passwords.

6 **Dangerous ICS/SCADA DNP3 function code sent to an RTU:** There are a number of built in function codes that identify the health of the assets at the grid's edge. These codes help determine the health of the assets and can be used to detect a number of man-in-the middle attacks. In both cases, the NSM tool accurately captured and logged these events.

7 **Malformed ICS protocol packet sent to master:** These packets indicate advanced levels of spoofing. Since the NSM tool is aware of the utilized control system protocols, it was able to detect a variety of malformed packets.

8 **Port scanning or other network profiling activities:** As demonstrated by Industroyer, the first malware specifically designed to attack power systems, trusted devices can become rogue and start initiating port scans [7]. This attack demonstrated the need to be able to detect any port scanning, even though these actions may originate from a device that is already located within the trusted control system network.

9 **IP spoofing and ARP poisoning:** There are several control system protocols and devices that are vulnerable to advanced levels of spoofing and ARP poisoning. By examining each communication packet at multiple layers of the OSI model, the NSM tool was able to alarm on these events.

10 **Anomalous utility operator activities (either intentional or accidental):** Since the tested NSM tool can be configured to be contextually aware of the control application and already understands the utilized protocols, triggers were created that monitor for suspicious or unrealistic operations. For instance, multiple back-to-back breaker open commands can be classified as suspicious activity and therefore warrant a notification. This type of event was also observed in the 2016 Ukraine cyberattack that resulted in the physical loss of power [7].

> "NSM can be used to increase the overall return on investment of the devices that are already installed in the field"

5. Approach Findings, Benefits and Event Grouping

When leveraged properly, network security monitoring offers substantial value beyond that of just cybersecurity. Other business units that can benefit from the information produced by a NSM tool include: **operational, compliance**, **asset management**, and **maintenance**. When utilized in this manner, NSM can be used to increase the overall return on investment of the devices that are already installed in the field, while also helping ease the burden across multiple departments. Table 1 shows 15 sample events or items that were automatically identified by the selected NSM tool. Though not an exhaustive list of all the tests performed, these examples demonstrate the breadth of information than can be captured and sent to various departments or business units. For example, the act of making a firmware change and the specific firmware version that is installed on a device has value for all four groups identified. The security team needs to know that the action is being performed, while the asset management and compliance teams need to know the final version that is installed. Operational personnel also will find this information helpful since it confirms any vendor features (like an added protection element) that may be used for future grid enhancements.

Example Item/ Event	Asset Management	Cybersecurity	Compliance	Operations
Device Serial Number	✓		✓	
Settings Changes	✓	✓	✓	
Firmware Changes	✓	✓	✓	✓
Network Mapping	✓	✓	✓	
Vulnerability Tracking	✓	✓	✓	
Whitelisting Alerts		✓		
Blacklisting Alerts		✓		
Failed Login		✓		
Active User		✓		
Port Scanning		✓		
Spoofing		✓		
Physical Entry		✓		
Protocol Errors		✓		✓
Repeated Control Commands		✓		✓
Time Synchronization Errors				✓

Table 1 Sample of Observed Items/Events and Information Categorization

6. Conclusion

Implementing network security monitoring in industrial control system networks provides asset owners the ability to leverage their existing infrastructure and investments to gain operational, compliance, asset inventory, network, and cybersecurity benefits. By extracting intelligence from device communications, ICS asset owners can configure their existing assets to become “cyber aware” by enabling built in features often not utilized or unknown to them. By stepping through a series of use case scenarios, this work demonstrated the utilization of technology for the extraction of security, compliance, operational, and asset management information. Given the passive nature of the developed approach, this work demonstrates how to safely extract this information in real-time, producing an efficient and feasible way of securing and managing the grid’s edge.

About the Authors

Nathan Wallace
Cybirical LLC

Nathan has a B.S. in electrical engineering, a B.S. in physics, a M.S. in engineering, and a Ph.D. in engineering cyberspace from Louisiana Tech University. He started his career with Entergy's relay settings and configuration group. He then joined a small utility as an associate engineer, performing field maintenance of system protection and communication equipment. After seeing the grid's growing reliance on cyber-based technologies, he pursued a graduate degree focusing on power system cybersecurity, where he also worked as a digital forensics examiner. Nathan currently is a staff engineer at Ampirical and a cofounder of Ampirical's sister firm Cybirical, where he is the Director of Cyber Engineering. He is a member of the IEEE Power & Energy Society (IEEE PES), Computer Society, and currently chairs two standard development groups in the IEEE PES Power System Communications & Cybersecurity (PSCC) Technical Committee.

Brian Proctor
Forescout

Brian has spent most of his career (13+ years) as a ICS/SCADA cybersecurity engineer and cybersecurity team lead working for two progressive California Investor Owned Utilities (IOUs). He holds a variety of technical certifications, including the Global Industrial Control System Professional (GICSP), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), and is certified in project management from University of California at Irvine. In 2013, Brian was presented with the Critical Infrastructure Private Sector award from Securing our eCity, a San Diego based cybersecurity non-profit organization. In 2016, Brian was a co-inventor of a R&D magazine top 100 award winner for one of the top inventions of the year relating to a GPS anti-spoofing mitigation technology

Want More Information?

To learn more about eyeInspect and its benefits for electric utilities, schedule a meeting with our cyber resilience experts at www.forescout.com/schedule-your-eyeinspect-demo/

[1] https://www.forescout.com/company/blog/largest-nerc-cip-fine-to-date/
[2] North American Electric Reliability Corporation (NERC), Standard: Critical Infrastructure Protection (CIP) https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[3] US Dept. of Homeland Security, "Recommended practice: Improving industrial control system cybersecurity with defense-in-depth strategies," 2009.
[5] Peter Bernus and Laszlo Nemes (1996) "A framework to define a generic enterprise reference architecture and methodology." Computer Integrated Manufacturing Systems Vol 9 (3) p. 179-191.
[6] IEEE Standard Std C37.240 -2014 "IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems." Approved 10 Dec. 2014.
[7] Anton Cherepanov, ESET "Win31/Industroyer – A New Threat for Industrial Control Systems." [Online] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com